CLAIMS

We claim:

1. A method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the method comprising the steps of:

obtaining intrusion information regarding an attack upon a device protected by an intrusion detection system;

obtaining network information regarding the attack upon the device; and

determining a portal of the attack upon the device by correlating the intrusion information and the network information.

2. The method of claim 1, wherein the portal of the attack is an entry point of the attack.

3. The method of claim 1, wherein the portal of the attack is an exit point of the attack.

4. A method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the method comprising the steps of:

obtaining intrusion information, from an intrusion detection system, regarding an attack upon a device protected by the intrusion detection system;

obtaining network information, from network equipment connected to the device, regarding the attack upon the device; and

determining a portal of the attack upon the device using a correlation engine to correlate the intrusion information and the network information.

5. A method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the method comprising the steps of:

obtaining intrusion information, from an intrusion detection system, regarding an attack upon a device protected by the intrusion detection system;

obtaining network information, from network equipment connected to the device, regarding the attack;

determining a logical entry point of the attack using a correlation engine to correlate the intrusion information and the network information; and

identifying a physical entry point associated with the logical entry point.

6. The method of claim 5, wherein the intrusion information includes an address.

7. The method of claim 5, wherein the address is a source address.

8. The method of claim 5, wherein the address is a destination address.

9. The method of claim 5, wherein the network information includes a logical port identifier of a logical port associated with the address.

10. The method of claim 9, wherein the step of determining a logical entry point includes the step of finding, in the network data, the logical port identifier of the logical port associated with the address.

11. The method of claim 9, wherein the step of identifying a physical entry point includes the step of identifying a physical port associated with the logical port.

12. The method of claim 5, wherein the network equipment includes a network router.

13. The method of claim 12, wherein the physical entry point includes a physical port of the network router.

14. The method of claim 12, wherein the logical entry point includes a logical port of the network router.

15. The method of claim 5, wherein the network equipment includes a firewall with routing function.

16. The method of claim 5, wherein the network equipment includes a network dispatcher.

17. The method of claim 5, wherein the network equipment includes a load balancer.

18. The method of claim 5, wherein the intrusion detection system includes network based intrusion detection equipment.

19. The method of claim 5, wherein the intrusion detection system includes host based intrusion detection equipment.

20. The method of claim 5, wherein the intrusion detection system includes application based intrusion detection equipment.